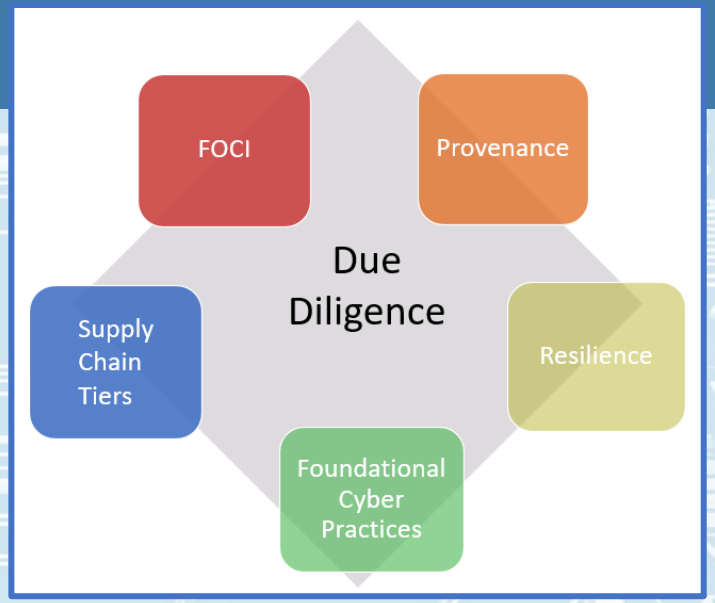
Check for updates

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Cybersecurity Supply Chain Risk Management

Due Diligence Assessment Quick-Start Guide



U.S. Department of Commerce
Howard Lutnick, Secretary
National Institute of Standards and Technology
Arvind Raman, NIST Director and Under Secretary of Commerce for Standards and Technology

NIST Special Publication
NIST SP 1326
https://doi.org/10.6028/NIST.SP.1326
July 2026

Background Information on this Quick-Start Guide

Certain open-source software tools are identified in this Quick-Start Guide to foster understanding. Such identification does not imply recommendation or endorsement by the National Institute of Standards and Technology, nor does it imply that the tools identified are necessarily the best available for the purpose.

Intended Audience

This publication is most useful for cybersecurity supply chain risk management (C-SCRM) practitioners both within a Program Management Office (PMO) capability as well as individuals with risk management responsibilities related to procurements. Familiarity with the below NIST Technical publications and selected concepts helps contextualize this Quick-Start Guide within NIST's broader guidance.

NIST Technical Publication	Concepts
Special Publication (SP) 800-39 *Managing Information Security Risk: Organization, Mission, and Information System View*	• Risk management strategy (Section 2.3.3, page 14) • Organizational risk tolerance (Section 2.3.3, page 14) • Multitiered risk management (Figure 2; page 9)
SP 800-53 Revision 5 *Security and Privacy Controls for Information Systems and Organizations*	• Difference between controls and requirements (Section 2.1, page 7) • How controls are organized (Table 1; page 8) and structured (Figure 1; page 9) • Employing a control catalog (Section 1.3, page 4) • Supply chain risk management controls (Section 3.20, page 363)
SP 800-161 Revision 1 *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*	• Cybersecurity risks throughout a supply chain (Introduction, page 1) • C-SCRM across organizational levels (Section 2.3.1, page 24) • Supply chain risk assessments (Section E.2, page 232) • Baseline risk factors, (Table 28, page 235)

If you are new to C-SCRM, it may help to learn from the above publications in the order listed. See also the "New to C-SCRM?" section of this document in the Learning Recap (page 18).

Table of Contents

Navigating This Quick-Start Guide

Due Diligence Assessment: Introduction

Purpose

This guide provides C-SCRM practitioners with considerations for creating due diligence supply chain risk assessments in accordance with NIST SP 800-161 Revision 1. It is a supplement to the content within SP 800-161 Revision 1 and is not intended to replace it.

What is Due Diligence in C-SCRM?

C-SCRM due diligence is the investigative process of researching and verifying all available, pertinent information about a given supplier or product so that informed decisions can be made on new acquisitions or existing systems. Due diligence refers to the minimum amount of reasonable research than an acquirer should conduct on a supplier. It should be done with most of the acquiring organization's suppliers, prioritized by criticality, prior to a more fulsome supplier review.

Basic vs. Enhanced Due Diligence

Basic due diligence is desktop-based research using publicly available information (PAI) to derive findings, as opposed to contacting suppliers requesting information. The use of commercial datasets, proprietary sources, and supply chain illumination tools (artificial intelligence-driven analytics platforms offering deeper supply chain visibility) constitutes enhanced due diligence. While some findings categories can be satisfactorily sourced using PAI, others may yield additional or faster results using enhanced toolsets. Organizations determine the level of due diligence based on available resources and acquisition criticality. All findings, regardless of source origin, should be validated against multiple sources when possible.

Scope of Due Diligence Assessment Quick Start Guide

Due diligence supplier assessments can be applied to any type of supplier, but this Quick-Start Guide is scoped to information and communications technology (ICT) suppliers.

EXPLORE MORE NIST C-SCRM RESOURCES

NIST C-SCRM Project

- ✓ SP 800 161r1
- ✓ C-SCRM Fact Sheet
- ✓ Federal C-SCRM Forum
- ✓ Software and Supply Chain Assurance Forum

Cybersecurity Framework 2.0 C-SCRM Quick-Start Guide

FIRST STEPS

Pre-Checks and Traceable Company Information

Research Considerations

Pre-Checks: Before You Start

Consider checking the following sources for a snapshot of U.S. Government (USG) regulatory concerns, prohibitions, and exclusions to potentially alleviate the need for further research.

- International Trade Administration (ITA)'s Consolidated Screening List: A list of entities for which the USG maintains restrictions on certain exports, reexports, or items transfers.
- System for Award Management (SAM)'s entity exclusions from USG procurement actions; sanctions, restrictions, and prohibitions; and ineligibility to contract with the USG.
- Supplier Performance Risk System's company exclusion status for Department of Defense acquisition professionals, including debarments and suspensions.

Traceable Company Information Examples

The following data points are generally available in the public domain or via SAM:

Company's Legal Name	Public/Private Status	Company Description	Incorporation Date and Location
Headquarters Address	Stock Ticker Symbol	DUNS Number	Employee Number
Website Address	For Profit/Nonprofit or Academic Status	Unique Entity Identifier	Office Locations

Link to SP 800-161r1 and Related Resources

Additional Company Information Considerations

The following data points and questions can augment your due diligence efforts:

Contracting Data Points	
Number of contracts within [date range]	
Dollar amount obligated within [date range]	
Specific agencies issuing contracts	
Presence of company products in subcontracts	

Security Clearance Questions	
Does the company participate in the National Industrial Security Program (NISP?)	
What is the company's Facilities Clearance (FCL) level?	
What is the company's highest Employee Clearance level?	

Diving Deeper: Consistency Across Findings and Information Validation

Research may uncover conflicting findings and data points for traceable company information and other due diligence research categories. Consider validating against USG-derived sources and company-derived sources for the most up-to-date traceable company information and using multiple information sources to validate supplier claims.

Related Resources

- Bloomberg offers publicly available and neutral company descriptions without a sales pitch.
- OpenCorporates provides basic traceable company information.
- USASpending and the Federal Procurement Data System (FPDS) contain contracting data.
- SAM.gov and the NISP Central Access Information Security System (NCAISS) contain security clearance data but require specialized permissions to review it.

NIST Due Diligence Assessment Quick-Start Guide:

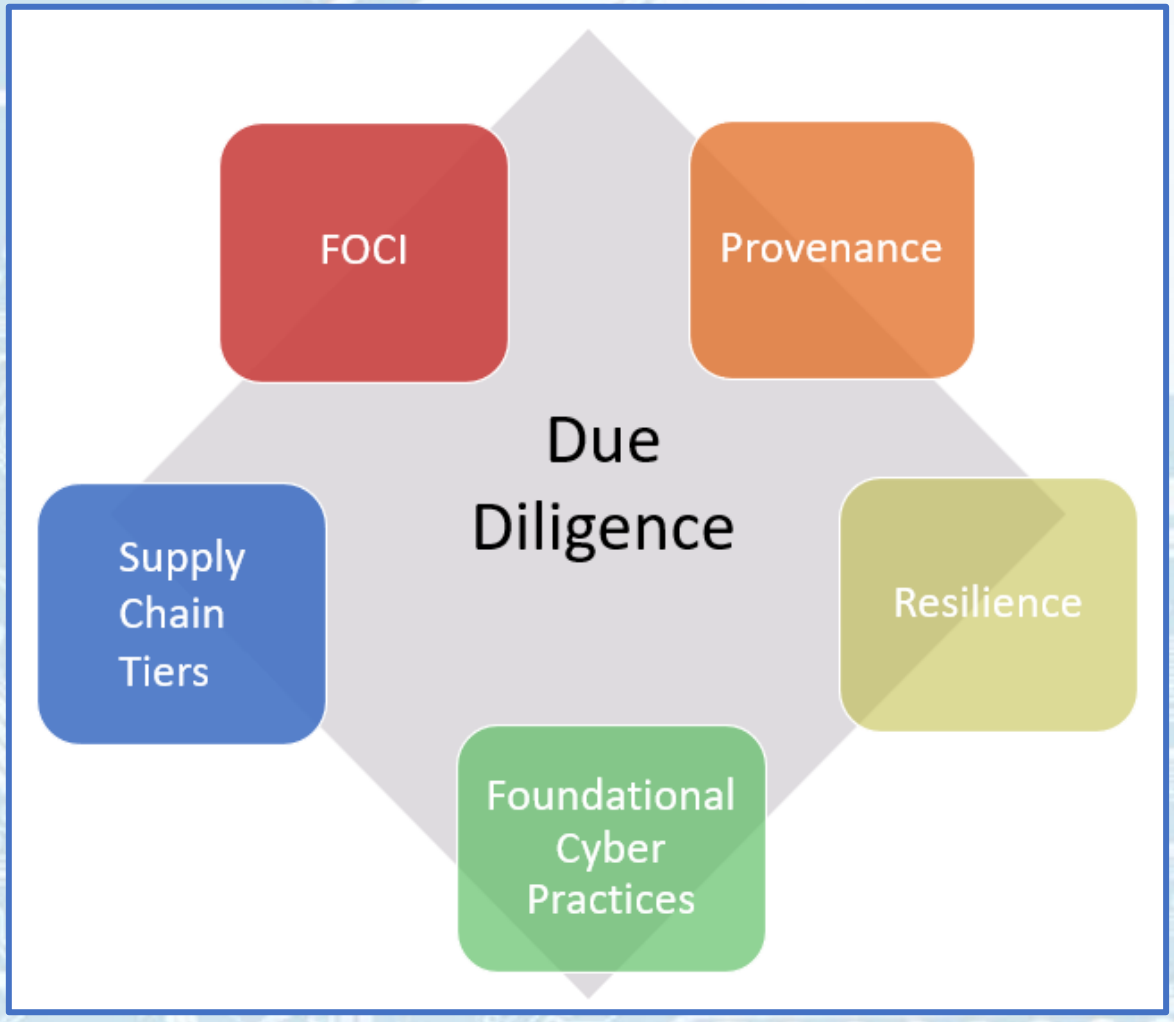
Due Diligence Research Categories

Overview: Research Categories

Due Diligence research includes five categories*:

1. Foreign Ownership, Control, or Influence (FOCI);
2. Provenance;
3. Resilience;
4. Foundational Cyber Practices; and
5. Supply Chain Tiers

*These categories are derived from the baseline risk factors in SP 800-161's Appendix E. For a more comprehensive list of risk factors, see Table 28 (p.235).



FOCI

Foreign Ownership, Control, or Influence

Research Considerations

Due Diligence FOCI Definition

- FOCI considerations for a supplier constitute significant ties to governments or government-controlled interests outside of the designated focal country with the power to affect the company's management or operations.
- Understanding suppliers' foreign ties helps determine risk derived from organization-defined countries of concern or adversary nations.

Ownership

- A foreign government holds [organization-defined] significant, ultimate, beneficial, or institutional ownership stake in the supplier, allowing that entity to influence policies and/or organizational or supply chain decisions that the supplier makes.

Key Leadership

- Executive-level leadership and/or supply chain leadership have [organization-defined] significant ties to foreign governments.

Foreign Laws, Policies, and Regulations

- Some nations have legal requirements for entity sharing with their security services, even for products and services that are not under their direct ownership, control, or influence.
- Sharing can encompass intellectual property, source code, design schematics, customer data, or other sensitive proprietary information as a prerequisite for conducting business within the foreign nation.
- Caveat: minimal investigation may extend beyond government FOCI into non-commercial entity partnerships, including geopolitical and regulatory relationships.

Key Questions

The following considerations can assist in developing FOCI questions to focus research:

Ownership/Control	
Does this company have foreign ownership, investment, or headquarters?	
Is the company undergoing an impending foreign merger or acquisition?	

Influence	
What SCRM-relevant key leaders have ties to foreign governments?	
Is the company subject to laws of sharing and cooperation with foreign security services?	

Levels of Concern can be assigned to Findings based on the organization's risk tolerance and system criticality. These are organization-defined levels of potential risk that can be identified using the methodology in SP 800-30, Guide for Conducting Risk Assessments.

Diving Deeper: Organization-Defined Parameters

Individual organizations will need to define their own system of trust regarding FOCI elements.

- Which countries are considered low, moderate, or high risk?
- How much foreign exposure can the organization tolerate in its critical suppliers?
- Can FOCI findings of concern be mitigated?

Related Resources

- Department of Commerce Foreign Adversaries List
- Department of State Countries of Concern

PROVENANCE

Place of origin for a supplier's operations or specific product development

Research Considerations

Due Diligence Provenance Definition

- Chronology of the origin, development, ownership, location, and changes to a system or system component, associated data, personnel, and services (SR-4), including analyses of component and subcomponent inventories (e.g., hardware and software bills of materials)
- Note: Per SR-4, *Pedigree* is the validation of provenance with evidence.

Supplier Operational Locations

- Research and development laboratories or locations of key source-code developers
- Manufacturing facilities, including factories and fabrication sites
- Assembly (i.e., where product subcomponents are put together)
- Testing and quality control
- Warehousing and storage (both physical facilities and virtual data servers)
- Shipping, distribution, and logistics nodes (e.g., air, land, and sea transportation)

Product-Specific Locations

- Findings specific to a particular product, component, or subcomponent
- For hardware, publicly available provenance locations at the country level, including manufacturing or assembly locations
- For software, open-source and third-party source code along with proprietary code development
- Third-party vendor or reseller supply chain

Link to SP 800-161r1 and Related Resources

Provenance Research Sources

The following resources can assist in identifying the key locations in a company's supply chain operations or the provenance of an individual product via publicly available information:

Supplier Sources	Hardware Sources	Software Sources
• Company-derived material (e.g., website, press releases, blog posts, legal policy) • Annual Securities and Exchange Commission (SEC) filings	• Company-provided datasheets • Online marketplace listings and product photos	• Company-provided software license documentation • Source-code repositories and binary files (e.g., for open-source software) • Software bills of materials (SBOMs)

Levels of Concern can be assigned to Findings based on organization-defined risk tolerance derived from the parameters used for FOCI.

Diving Deeper: Subcomponents

- Provenance research also encompasses the supply chain of critical product subcomponents.
- To scope research for hardware, consider whether logic-bearing components store, send, save, assess, or transmit data.
- SBOMs should only be produced using NTIA-supported formats that can satisfy EO 14028 minimum elements as framing for the inclusion of primary components. They should be digitally signed using a verifiable and trusted key.
- Subcomponents may be made in one country with a different assembly country being listed as the "country of origin."

Related Resources

- NTIA: The Minimum Elements for a Software Bill of Materials

RESILIENCE

Findings that impact the reliability, regulatory compliance, or authenticity of a supplier or product

Research Considerations

Due Diligence Resilience Definition

- Information that potentially impacts the ability of a supplier to meet contractual obligations, including product reliability, supplier compliance with government regulations, and the presence of counterfeit devices in the market space

Organizational Resilience Concerns

- Financial distress (e.g., bankruptcies, credit insolvency, significant debt, risky investments)
- Legal difficulties (e.g., significant lawsuits/litigation, particularly those related to product stability; instances of industrial theft or espionage)
- Leadership turnover for key executive positions
- Regulatory violations (e.g., export controls, International Traffic in Arms Regulations (ITAR), Foreign Corrupt Practices Act, government exclusions)
- Known associations with terrorist or criminal elements
- Data breaches, including ransomware
- Use of conflict materials or forced labor
- Environmental instability in key operational locations

Product Resilience Concerns

- Customer reports of poor product performance
- Known instances of counterfeiting or unauthorized white-labeling
- Known instances of a supplier frequently showing willful negligence or deploying intentionally malicious practices that can degrade the customer's level of trust in its products

Regulatory Compliance Lists

The following entities represent various USG prohibitions that may be useful in identifying government exclusions of suppliers or their key personnel:

- FY99 National Defense Authorization Act (NDAA) Section 1237
- FY19 NDAA Section 889
- FY21 NDAA Section 1260H
- FY23 NDAA Section 5949
- FCC's SECURE Networks Act Covered List
- ITA's Consolidated Screening List

Levels of Concern can be assigned to Findings based on organization-defined risk tolerance.

Diving Deeper: Historical Data vs. Relevant Information

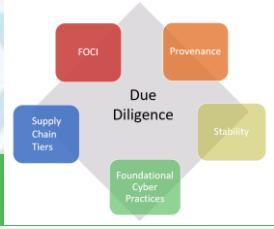
Organizations define their own levels of risk tolerance specific to individual research findings for the following variables:

- Age of the information found
- Frequency of event occurrence
- Severity of research finding
- Supplier mitigations currently (or not) in place to prevent reoccurrence

Related Resources

- System for Award Management
- National Vulnerability Database
- ACT-IAC: Identification and Use of Restricted and Sanctioned Entity Lists

FOUNDATIONAL CYBER PRACTICES 1



Part 1: Overall cybersecurity posture of a supplier's information technology assets

Research Considerations

Due Diligence Foundational Cyber Practices: Part 1 — Securing the Supplier

- Findings regarding the cyber health of the supplier's information technology (IT) assets to measure its ability to deliver on promised services and safeguard sensitive data.

System Compromises

- Malware infections, including server and botnet compromises
- Spam propagation (i.e., automated distribution of large amounts of unsolicited communications deriving from the entity)

User Behavior

- Exposed credentials from third-party data breaches
- Insecure BitTorrent protocol file sharing

Security Posture

- Unnecessary open ports
- Vulnerability patching cadence
- Mobile application security
- Endpoint/configuration security
- Presence of obsolete software versions
- Susceptibility to ransomware attacks or business interruption
- Unwanted functionality

Spotlight on Data Breaches

Incidences of data breaches exposing a company's internal information, including proprietary or customer data, can be often be found via a basic search engine check. When assessing the ramifications of a data breach or successful cyber attack against a supplier, consider the following questions:

- How long ago was the incident?
- What did the incident entail, and what was the severity of the impact?
    - For example: Credentials stolen, sensitive data compromised/exfiltrated, denial of service.
- Did the breach impact the confidentiality, integrity, or availability of the supplier's products or the data stored within the supplier's networks?
- What steps did the supplier take to mitigate the attack's impact and prevent future occurrences?

Technical Deep Dive: NIST Computer Security Incident Handling Guide

Where to Find Information

Some aggregated information about supplier IT assets is not available on the open web and may require the use of an illumination tool for analytics, such as:

- Domain Name Services Checker (DNSChecker) and Robtex provide a basic and open-source overview of a website's metadata.
- Shodan is a search engine for internet-connected devices that can give a footprint of a supplier's network.
- HackerTarget offers multiple free tools for DNS health checks, IP geolocation, port scanning, network tests, and web tools.
- VirusTotal offers malware detection and analysis for URLs, files, domains, and IPs.
- Free Secure Socket Layer (SSL) grading websites like Qualys SSL Labs Scanner or Mozilla Observatory offer analysis for web server SSL configurations.

FOUNDATIONAL CYBER PRACTICES 2

Part 2: Secure product development and product-specific cybersecurity concerns for software and firmware

Research Considerations

Due Diligence Foundational Cyber Practices: Part 2 — Secure Product Development

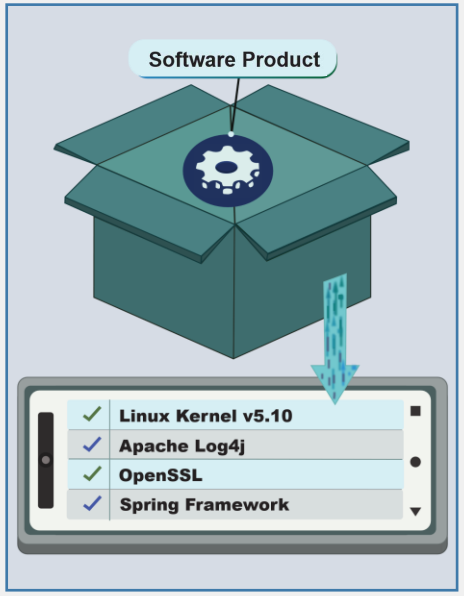
- Supplier's use of cybersecurity key practices when developing products as well as product-specific concerns that cause offerings to not operate as the manufacturer originally intended, including software and firmware found in hardware products

Publicly Available Product Findings

- Unpatched Common Vulnerability Exposures (CVEs)
- Product lifespan (e.g., end-of-life considerations, cessation of security updates, product maturity)
- Update/upgrade frequency, including latest available product version

Software Bill of Materials (SBOM) Considerations

- A software bill of materials is a formal record containing the details and supply chain relationships of various components used in building software, including open-source and third-party dependencies.
- Having a SBOM does not automatically mean the software is secure but allows for a more tailored risk assessment based on knowledge of its subcomponents.
- Machine-readable SBOMs in standard formats such as CycloneDX, SPDX, and SWID allow for automated ingesting, validation, and analytics.



SBOM Analytics Findings

- Who has contributed code or modifications to each subcomponent; potentially validating via cryptographic hash, signature, or digital certificate? Can include presence (percentage and analytics) of committers with FOCI concerns.
- Sole-source committers: dependencies or subcomponents that rely on a single individual or a small number of contributors for updates, maintenance, and patches
- Prioritization of dependencies by criticality to overall system security.
- Level of community support and engagement for subcomponents, including maintenance/update frequency (i.e., how often the subcomponent/dependency source code is revised or modified)
- Subcomponent end-of-life considerations, including age of subcomponent.
- Presence (percentage and analytics) of known vs. unknown subcomponents.
- Known unpatched and/or exploited CVEs in subcomponents or dependencies, as well as historical compromises.

Supplier Software Attestation Updates

- OMB M-26-05 rescinded the mandate that federal agencies require software developers to attest they have followed Secure Software Development Framework (SSDF) practices per OMB M-22-18 and M-23-16, instead favoring tailoring assurance requirements to individual agencies.

Related Resources

- SP 800-218, Secure Software Development Framework
- SP 800-160v2r1, Developing Cyber Resilient Systems
- 2025 Minimum Elements for a SBOM

SUPPLY CHAIN TIERS

Organization of suppliers into levels based on relationship to the end user

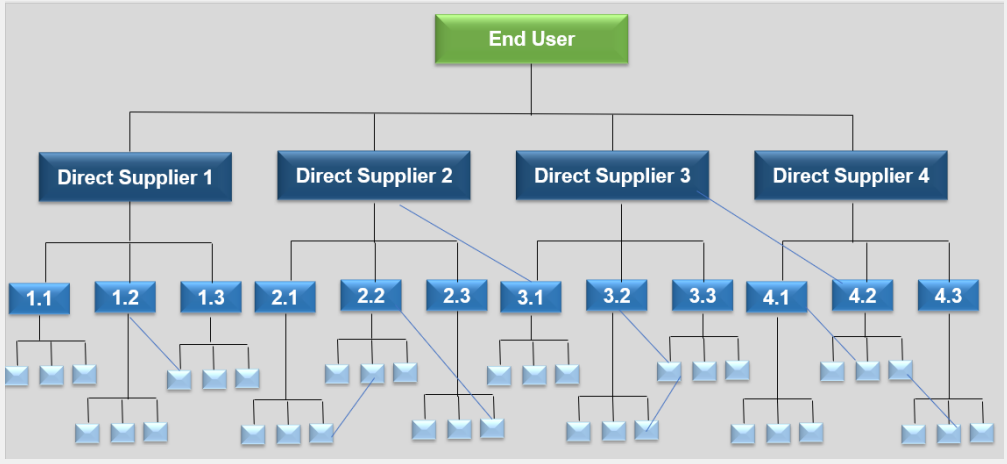
Research Considerations

Due Diligence Supply Chain Tiers Definition

- Suppliers are organized into tiers based on their relationship to the end user.
- First-tier suppliers provide products and/or services directly to the end user.
- Second-tier suppliers provide products and/or services to first-tier suppliers.
- The tiers can go down to X level, depending on organizational preference. Going down further in the supply chain tier structure increases one's visibility and understanding, but the difficulty and cost exponentially increase.

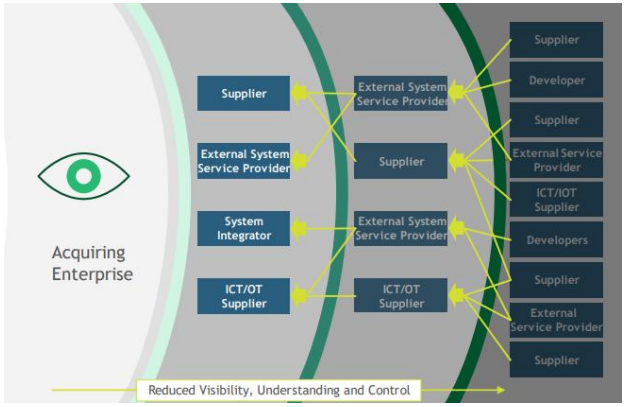
Illuminating the Supply Chain Tier Structure with Tools

- Researching with supply chain illumination tools can help visualize the organization or program's supply chain tier structure, identify commonalities and relationships across suppliers, and potentially provide insight into supplier concerns. Corroborating findings across publicly available information (PAI) or multiple tools ensures greater accuracy.



Due Diligence Considerations on Supply Chain Tiers

- Supplier presence on regulatory compliance lists, watchlists, or USG exclusion lists (see Resilience)
- FOCI concerns with direct and sub-tier suppliers
- Organization-defined concerns with direct and sub-tier suppliers (e.g., foreign defense and aerospace entities that are direct suppliers of programs that support national security systems)



Sub-Tier Supplier Diversity

- The further one gets from the end user, the larger the supplier portfolio becomes, increasing the corresponding likelihood of supplier presence on an exclusion list, watchlist, or regulatory noncompliance list.

Questions to Consider

- Analyzing the supply chain tier structure can illuminate sole source supplier concerns. Do multiple direct suppliers all rely on the same sub-tier suppliers? Does sole sourcing to a trusted entity mitigate concerns with problematic suppliers?
- What is your organization's risk tolerance for FOCI concerns with direct and sub-tier suppliers?
- How should your organization's risk tolerance balance the risks of limited supplier diversity with the increased likelihood of watchlisted suppliers in the sub-tier portfolio?

Related Resources

- NIST IR 8179, Criticality Analysis Process Model

NIST Due Diligence Assessment Quick-Start Guide:

Due Diligence in Context

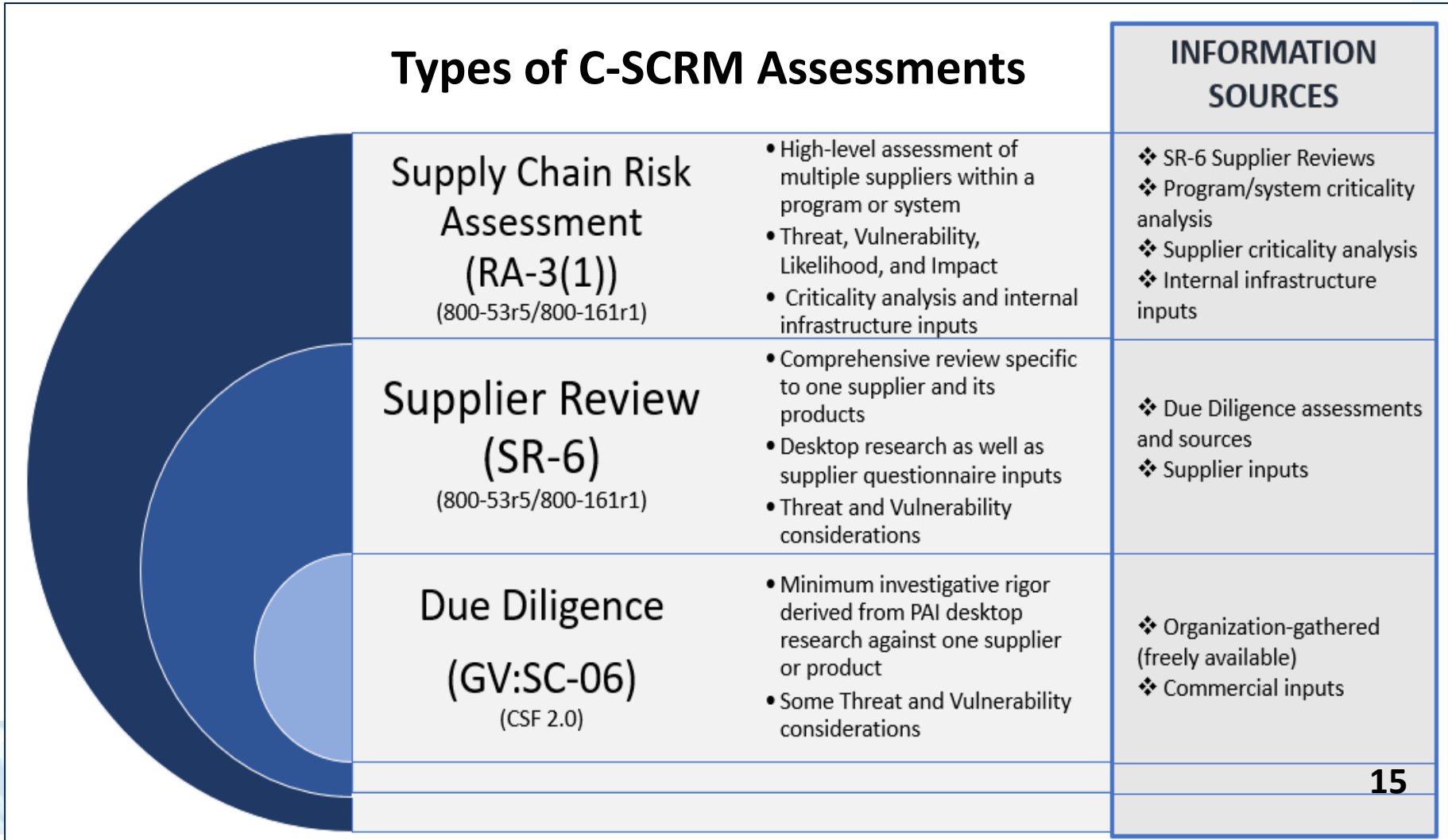
Due Diligence, Supplier Reviews, and SCRAs: Relationship to SR-6 and RA-3(1)

Due Diligence and Supply Chain Risk Assessments (SCRA)

Per SP 800-161r1, the C-SCRM Program Management Office (PMO), PMO capability, or individual responsible for C-SCRM conducts assessments of cybersecurity risks arising from suppliers seeking to integrate products or services with a given system in accordance with enterprise-wide C-SCRM policy requirements. SP 800-161r1 shows that **Cybersecurity Risk** is the **Likelihood** of **Threats** exploiting **Vulnerabilities** and causing an **Impact** to a program or system.

Due Diligence Assessments are a precursor to the SR-6 Supplier Reviews and, in many cases, can serve as the foundation of the Threat and Vulnerability aspects of the more robust RA-3(1) Supply Chain Risk Assessment. The graphic to the right Illustrates three types of C-SCRM assessments – beginning with due diligence as a foundational step.

Due diligence assessments can be researched and written using PAI, as well as augmented with commercially derived datasets and illumination tools. The components of a Due Diligence Assessment are **Foreign Ownership, Control, or Influence (FOCI); Provenance; Resilience; Supply Chain Tiers; and Foundational Cyber Practices.**



Due Diligence Findings and Classification

Classifying Due Diligence Findings

While this guidance discusses publicly available information and findings that are derived from publicly available research or commercially derived datasets in the public domain, organizations need to determine what classification the aggregation of findings and individual findings should hold, if any.

- Findings that aggregate vulnerabilities in information systems for National Security Systems (NSS) and other programs resident on classified systems should follow the appropriate Security Classification Guide for classification markings. For programs that are not resident on NSS or classified systems, consider marking documents that aggregate vulnerability findings as Controlled Unclassified Information (CUI) to protect vulnerability information.
- Consider marking individual findings that are derived from commercial illumination tools or those that require login credentials or special roles/access within government systems as CUI to protect those sources' proprietary business information.

Additional Resources

- The National Archives and Records Administration Controlled Unclassified Information Categories provide federal-level guidance on CUI policies and practices for specific subsets of CUI.
- SP 800-171r3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, provides recommended security requirements for protecting the confidentiality of CUI.
- SP 800-161r1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, provides guidance on identifying, assessing, and mitigating cybersecurity risks throughout the supply chain at all levels of an organization.
- The NIST Cybersecurity and Privacy Reference Tool (CPRT) provides reference data from various NIST cybersecurity and privacy standards, guidelines, and frameworks in common downloadable formats (e.g., XSLS and JSON).
- SP 800-53r5, Security and Privacy Controls for Information Systems and Organizations, provides a catalog of security and privacy controls for which SP 800-161r1 offers additional enhancements that are specific to C-SCRM. The controls are flexible, customizable, and implemented as part of an organization-wide process to manage risk. View and export information from the Cybersecurity and Privacy Reference Tool (CPRT).
- MITRE's System of Trust™ is a freely available public framework designed to standardize and improve the assessment of supply chain security risks by providing a consistent method to identify, evaluate, and mitigate potential risks across an organization's suppliers and services.

NIST Due Diligence Assessment Quick-Start Guide:

Learning Recap

REVIEW: LEARNING RECAP

Summary of the key concepts in this Due Diligence Assessment Quick-Start Guide

What We Learned. This QSG explained the following:

- **Due diligence in cybersecurity supply chain risk management (C-SCRM)** — The process of researching and verifying all available, pertinent information about a given ICT supplier or product.
- **Due diligence research considerations** — *First Steps* (pre-checks and traceable company information); *Supply Chain Tiers* (organizing suppliers into levels based on their relationship to the end user); *Foreign Influence, Control, or Ownership (FOCI)*; *Provenance* (place of origin for the supplier's general operations or a specific product); *Resilience* (findings that impact the reliability, regulatory compliance, or authenticity of a supplier or product); and *Foundational Cyber Practices* (overall cybersecurity posture of a supplier's public-facing information technology assets and cybersecurity concerns for hardware, software, and product development) to ensure that informed decisions can be made about whether to enter into contracts and agreements.
- **Supply chain risk assessments (SCRA) —** Assessments of cybersecurity risks that arise from business partners seeking to integrate with a given system.

What's Next. Here are some things you can do to put this QSG into practice:

1. **Develop a Due Diligence Report template** that includes findings for research and sources to find and verify information (both PAI and commercially provided).
2. **Define levels of concern for findings**. Use your organization's baseline risk tolerance to develop a rating schema that determines when findings rise to a level of concern that constitutes risk.
3. **Consider a continuous monitoring process.** Determine when information should be refreshed and develop a process (manual or automated) to update reports.

This QSG provides an overview of C-SCRM due diligence. It is a supplement to SP 800-161r1 and is not intended to replace it.

New to C-SCRM?

These NIST resources can help you understand the basics of C-SCRM and complete your due diligence assessments:

- NIST's Cybersecurity SCRM Fact Sheet provides a brief but substantive introduction to C-SCRM.
- SP 800-161r1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, helps organizations identify, assess, and respond to supply chain risks at all levels. Appendix A identifies the C-SCRM-related controls from SP 800-53r5, augments those controls with additional supplemental guidance, and provides new controls as appropriate.
- SP 1305, Cybersecurity Framework 2.0 C-SCRM Quick Start Guide, offers guidance on establishing a C-SCRM capability and using the CSF to communicate supplier requirements.
- NIST IR 8179, Criticality Analysis Process Model, helps organizations identify systems and components that are most vital and which may need additional security or other protections.
- The Federal C-SCRM Forum fosters collaboration and the exchange of C-SCRM information among federal organizations to improve the security of federal supply chains.
- The Software and Supply Chain Assurance Forum provides a venue for government, industry, and academic participants from around the world to share their knowledge and expertise regarding C-SCRM, supply chain risks, effective practices and response strategies, tools and technologies, and any gaps related to the people, processes, or technologies involved.

NIST Due Diligence Assessment Quick-Start Guide: *Glossary*

GLOSSARY

Definitions of key terms in this Due Diligence Assessment Quick-Start Guide

- **Basic due diligence:** Desktop-based research using publicly available information (PAI) to derive due diligence findings.
- **Due diligence:** The investigative process of researching and verifying all available, pertinent information about a given supplier or product so that informed decisions can be made on new acquisitions or existing systems.
- **Enhanced due diligence:** The use of commercial datasets, proprietary sources, and supply chain illumination tools to derive due diligence findings.
- **Foreign ownership, control, or influence (FOCI):** Significant ties to governments or government-controlled interests outside of the designated focal country with the power to affect a company's management or operations.
- **Provenance:** Chronology of the origin, development, ownership, location, and changes to a system or system component, associated data, personnel, and services (SR-4), including analyses of component and subcomponent inventories (e.g., hardware and software bills of materials).
- **Resilience:** Information that potentially impacts the ability of a supplier to meet contractual obligations, including product reliability, supplier compliance with government regulations, and the presence of counterfeit devices in the market space.

The definitions in this glossary are meant to inform research in the context of C-SCRM and due diligence. They are not intended to be used as holistic, stand-alone definitions outside of that context.

NIST CSRC Glossary

NIST's Computer Security Resource Center (CSRC) contains a glossary that aggregates terms and definitions specified in NIST's cybersecurity and privacy standards, guidelines, and other technical publications, as well as other official sources, including U.S. laws, the Code of Federal Regulations, Presidential Directives, and the Committee for National Security Systems.

Users of this Quick-Start Guide may consult the CSRC Glossary for variations of these terms that may exist in other contexts.

The Glossary is available at: https://csrc.nist.gov/glossary.

CONTACT NIST

About C-SCRM

Website:
https://csrc.nist.gov/projects/cyber-supply-chain-risk-management

Email:
scrm-nist@nist.gov

Google Group:
sw.assurance@list.nist.gov

Forum:
https://csrc.nist.gov/Projects/cyber-supply-chain-risk-management/ssca